

WE CLAIM:

1 1. A method of controlling a security association of a network communication between
2 a local application and a remote application, the local application utilizing a socket, said method
3 comprising:

4 (a) monitoring a completion status of the communication;

5 (b) upon completion of the communication, closing the socket; and

6 (c) in response to closing of the socket, terminating a correlation of the security
7 association with the socket.

1 2. A method as claimed in claim 1, wherein step (c) comprises deleting the security
2 association.

1 3. A method as claimed in claim 1, wherein step (c) comprises determining whether any
2 other socket is correlated with the security association, and when it is determined that no other
3 socket is correlated with the security association, deleting the security association.

1 4. The method of claim 1, wherein the application operates through a driver, and step (c)
2 includes notifying the driver that the security association is no longer needed, to cause the driver
3 to terminate the correlation.

1 5. A method of controlling communication between a local application and a remote
2 application on a communication network, said method comprising:

3 (a) creating a socket for the local application;

4 (b) correlating the socket with a security association;

5 (c) performing the communication through the socket and the communication network;
6 (d) upon completion of the communication closing the socket; and
7 (e) in response to closing of the socket, terminating the correlation of the security
8 association with the socket.

1 6. The method of claim 5, wherein step (b) comprises:

2 (1) determining whether there is an active security association that would cover traffic for
3 the socket;

4 (2) if step (1) determines that there is an active security association that would cover
5 traffic for the socket, then correlating the socket with the active security association;

6 (3) if step (1) determines that there is not an active security association that would cover
7 traffic for the socket, then:

8 (i) determining a security association for traffic for the socket;
9 (ii) giving the determined security association to a network security driver;
10 (iii) receiving a handle for the security association from the network security
11 driver; and

12 (iv) correlating the socket with the security association of the handle.

1 7. A method as claimed in claim 5, wherein step (e) comprises deleting the security
2 association.

1 8. A method as claimed in claim 5, wherein step (e) comprises determining whether any
2 other socket is correlated with the security association, and when it is determined that no other
3 socket is correlated with the security association, deleting the security association.

1 9. The method of claim 5, wherein the application operates through a driver, and step (e)
2 includes notifying the driver that the security association is no longer needed, to cause the driver
3 to terminate the correlation.

1 10. A security system for connecting a client application to a communication network,
2 wherein said security system comprises:

3 a transmission control protocol for controlling communication between the client
4 application and the communication network;

5 a security classifier for coupling said transmission control protocol to the network, said
6 security classifier determining a security classification for the client application;

7 a security association negotiator responsive to the client application opening a socket at
8 a node of the communication network, for correlating the socket with a security association based
9 on the determined security classification; and

10 a network interceptor coupling the client application with the transmission control
11 protocol, and responsive to the socket being closed for terminating the correlation of the socket
12 with the security association.

1 11. A security system as claimed in claim 10, wherein the network interceptor responds
2 to the socket being closed by deleting the security association.

1 12. A security system as claimed in claim 10, wherein the network interceptor responds
2 to the socket being closed by determining whether any other socket is correlated with the security

3 association, and when it is determined that no other socket is correlated with the security
4 association, deleting the security association

5b
A'

1 13. A communication system, comprising:
2 a communication network, including a plurality of nodes;
3 a server connected to a first one of said nodes;
4 a client processor;
5 a storage medium within said client processor and storing a security system for connecting
6 said client processor to said communication network for communication with said server, wherein
7 said security system includes a transmission control protocol for controlling communication
8 between said client processor and said communication network; a security classifier for coupling
9 said transmission control protocol to said communication network, said security classifier
10 determining a security classification for said client processor; a security association negotiator
11 responsive to said client processor opening a socket at a node of said communication network,
12 for correlating the socket with a security association based on the determined security
13 classification; and a network interceptor coupling said client processor with said transmission
14 control protocol, and responsive to the socket being closed for deleting the security association.

1 14. A communication system as claimed in claim 13, wherein the network interceptor
2 responds to the socket being closed by deleting the security association.

1 15. A communication system as claimed in claim 13, wherein the network interceptor
2 responds to the socket being closed by determining whether any other socket is correlated with

the security association, and when it is determined that no other socket is correlated with the security association, deleting the security association.

16. An article, comprising a storage medium having instructions stored thereon, the instructions when executed controlling a security association of a network communication between a local application and a remote application, the local application having a socket, by monitoring a completion status of the communication; upon completion of the communication, closing the socket; and in response to closing of the socket, terminating a correlation of the security association with the socket.

17. An article as claimed in claim 16, wherein the correlation of the security association with the socket is terminated by deleting the security association.

18. An article as claimed in claim 16, wherein the correlation of the security association with the socket is terminated by determining whether any other socket is correlated with the security association, and when it is determined that no other socket is correlated with the security association, deleting the security association.

19. An article as claimed in claim 16, wherein the application operates through a driver, and the correlation of the security association with the socket is terminated by notifying the driver that the security association is no longer needed, to cause the driver to terminate the correlation.

Add A2